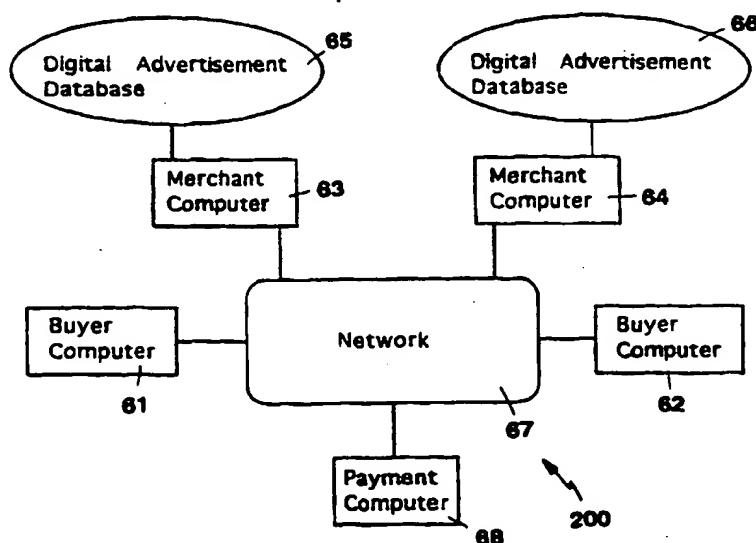


PCTWORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : G06F 157/00		A1	(11) International Publication Number: WO 95/16971
			(43) International Publication Date: 22 June 1995 (22.06.95)
(21) International Application Number: PCT/US94/14319			(81) Designated States: JP, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).
(22) International Filing Date: 13 December 1994 (13.12.94)			
(30) Priority Data: 08/168,519 16 December 1993 (16.12.93) US			
(71) Applicant: OPEN MARKET, INC. [US/US]; 215 First Street, Cambridge, MA 02141 (US).			
(72) Inventor: GIFFORD, David, K.; 26 Pigeon Hill Road, Weston, MA 02193 (US).			
(74) Agent: WALPERT, Gary, A.; Fish & Richardson P.C., 225 Franklin Street, Boston, MA 02110-2804 (US).			Published <i>With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i>

(54) Title: DIGITAL ACTIVE ADVERTISING



(57) Abstract

A complete system (200) for the purchasing of goods or information over a computer network (67) is presented. Merchant computers (63, 64) on the network (67) maintain databases of digital advertisements (65, 66) that are accessed by buyer computers (61, 62). In response to user inquiries, buyer computers (61, 62) retrieve and display advertisements from merchant computers (63, 64). A digital advertisement can include a program that is interpreted by a buyer's computer (61, 62). The buyer computers (61, 62) allow the users to purchase the product described by an advertisement. The form of payment can be requested after a purchase is initiated. A payment system (300) performs payment authorization. The payment system obtains account authorizations from an external financial system. Payment orders are signed with authenticators.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	GB	United Kingdom	MR	Mauritania
AU	Australia	GE	Georgia	MW	Malawi
BB	Barbados	GN	Guinea	NE	Niger
BE	Belgium	GR	Greece	NL	Netherlands
BF	Burkina Faso	HU	Hungary	NO	Norway
BG	Bulgaria	IE	Ireland	NZ	New Zealand
BJ	Benin	IT	Italy	PL	Poland
BR	Brazil	JP	Japan	PT	Portugal
BY	Belarus	KE	Kenya	RO	Romania
CA	Canada	KG	Kyrgyzstan	RU	Russian Federation
CF	Central African Republic	KP	Democratic People's Republic of Korea	SD	Sudan
CG	Congo	KR	Republic of Korea	SE	Sweden
CH	Switzerland	KZ	Kazakhstan	SI	Slovenia
CI	Côte d'Ivoire	LI	Liechtenstein	SK	Slovakia
CM	Cameroon	LK	Sri Lanka	SN	Senegal
CN	China	LU	Luxembourg	TD	Chad
CS	Czechoslovakia	LV	Latvia	TG	Togo
CZ	Czech Republic	MC	Monaco	TJ	Tajikistan
DE	Germany	MD	Republic of Moldova	TT	Trinidad and Tobago
DK	Denmark	MG	Madagascar	UA	Ukraine
ES	Spain	ML	Mali	US	United States of America
FI	Finland	MN	Mongolia	UZ	Uzbekistan
FR	France			VN	Viet Nam
GA	Gabon				

- 1 -

DIGITAL ACTIVE ADVERTISING
BACKGROUND OF THE INVENTION

5 The recent rapid growth of information applications on international public packet-switched computer networks such as the Internet suggests that public computer networks have the potential to establish a new kind of open marketplace for goods and services.
10 Such a marketplace could be created with a network sales system that comprises a plurality of buyer and merchant computers, means for the users of the buyer computers to display digital advertisements from the merchant computers, and means for the users to purchase products
15 described by the advertisements.

 A network based sales system will need to allow users to preview products at little or no cost, and will need to make a large number of product advertisements available in a convenient manner. In addition, the
20 shopping system will need to include easy-to-use facilities for a user to purchase desired products using a merchant independent payment method. In addition the network sales will need to allow new buyers and merchants to enter the market.

25 A central requirement for a marketplace is a payment mechanism, but at present no merchant independent payment mechanism is available for computer networks that permits users to utilize conventional financial instruments such as credit cards, debit cards, and demand
30 deposit account balances. We expect that both retail payment and wholesale payment mechanisms will be required for networks, with consumers using the retail mechanism for modest size purchases, and institutions using the wholesale mechanism for performing settlement between
35 trading partners. For wide acceptance the retail mechanism will need to be a logical evolution of existing

- 2 -

credit-card, debit-card, and Automated Clearing House facilities, while for acceptance the wholesale mechanism will need to be an evolved version of corporate electronic funds transfer.

5 These problems of have been approached in the past by network based sales systems wherein, for example, each merchant maintains an account for each user. A user must establish an account with each merchant in advance in order to be able to utilize the merchant. The prior
10 art network based sales systems are not designed to allow users to use their existing credit card and demand deposit accounts for payment, nor are they designed to allow for programs to be included in digital advertisements.

15 According, therefore, it is a primary objective of this invention to provide a user interactive network sales system in which the user can freely use any merchant of choice and utilize existing financial instruments for payment. Other objects include a network
20 sales system which provides a high-quality user interface, which provides users with a wide variety and large volume of advertisements, which is easily extensible to new services, and which is easily expanded to new applications within the existing infrastructure of
25 the system.

 Still other objects of the invention are to provide a network payment system that will authorize payment orders and remove part of the risk of fraud from merchants.

30 An unavoidable property of public computer networks is that they are comprised of switching, transmission, and host computer components controlled by many individuals and organizations. Thus it is impossible for a network payment system to depend upon a
35 specified minimum required degree of software, hardware,

- 3 -

and physical security for all of the components in a public network. For example, secret keys stored in a given user's personal computer can be compromised, switches can be tampered with to redirect traffic, and
5 transmission facilities can be intercepted and manipulated.

The risk of performing retail payment in a public network is compounded by statutes that make a payment system operator in part liable for the security lapses of
10 its users. Existing Federal statutes in the United States, including the Electronic Funds Transfer Act and the Consumer Credit Protection Act, require the operator of a payment mechanism to limit consumer liability in many cases. Payment system operators may have other
15 fiduciary responsibilities for wholesale transactions. Similar responsibilities exist in other countries for retail and wholesale transactions.

In existing credit card payment systems, a credit card's issuing bank takes on the fraud risk associated
20 with misuse of the card when a merchant follows established card acceptance protocols. Acceptance protocols can include verifying a card holder's signature on the back of their card and obtaining authorization for payments over a certain value. However, in network based
25 commerce a merchant can not physically examine a purchasers credit card, and thus the fraud risk may revert to the merchant in so called "card not present" transactions. Many merchants can not qualify to take this risk because of their limited financial resources.
30 Thus the invention is important to allow many merchants to participate in network based commerce.

Other objects of the invention include utilizing existing financial instruments such as credit cards, debit cards, and demand deposit accounts for merchant
35 payments.

- 4 -

Existing network payment systems do not connect to the financial system for authorization and are not compatible with conventional financial instruments. Existing network payment systems include the Simple Network Payment Protocol [Dukach, S., SNPP: A Simple Network Payment Protocol, MIT Laboratory for Computer Science, Cambridge, MA, 1993.], Sirbu's Internet Billing Server [Sirbu, M. A., Internet Billing Service Design and Prototype Implementation, Information Networking Program, Carnegie-Mellon University, 1993], and NetCash [Medvinsky, G., and Newman, B. C., NetCash: A Design for Practical Electronic Currency on the Internet, Proc. 1st ACM Conf. on Comp. and Comm. Security, November, 1993].

A further object of the invention is to allow users in an untrusted network environment to use conventional financial instruments without requiring modification to existing financial system networks.

The following definitions apply to the present invention. A principal is a person, company, institution, or other entity that is authorized to transact business as part of a network payment system. A payment order describes the identity of a sender, a payment amount, a beneficiary, and a sender unique nonce.

A sender is a principal making a payment. A beneficiary is a principal to be paid by the payment system. A sender unique nonce is an identifier that is used only once by a given sender. An example of sender unique nonces are unique timestamps. An external account is an account that can be used to settle a payment order for either a sender or a beneficiary in the external financial system. Examples of external accounts include demand deposit accounts and credit card accounts. An external device is a physical object that is kept in the possession of a user for the purpose of identifying the user.

- 5 -

A network payment system is a service that authorizes and executes digital payment orders that are backed by external accounts. A payment system authenticates a payment order, checks for sufficient funds or credit, and then originates funds transfer transactions to carry out the payment order. A payment system acknowledges acceptance or rejection of a payment order. More than one payment system may exist on a given network, and a given payment system may operate on more than one host to increase its reliability, availability, and performance. An authenticator is a digital value that is appended to a payment order and becomes part of the payment order that authenticates the payment order as genuine.

15

SUMMARY OF THE INVENTION

The invention relates to a network sales system for enabling users to purchase products using a plurality of buyer computers that communicate over a network with a plurality of merchant computers. Each merchant computer has a database of digital advertisements. Each digital advertisement includes a price and a product abstract. Buyer computers request, display, and respond to digital advertisements from merchant computers. Users can purchase products with their buyer computers after they have specified an account to pay for the purchase. A network payment service is used to authorize the purchase before merchant fulfillment is performed.

In a particular aspect of the invention, the merchant computer can request account information when it is not provided by the buyer computer. In another aspect of the invention, the buyer computer can present to a merchant a pre-authorized payment order that is obtained from a network payment system.

In another aspect of the invention, an electronic sales system contains digital advertisements that include

- 6 -

programs. The programs are executed on behalf of a user by a buyer computer, and can lead to a purchase request directed to a merchant computer that performs product fulfillment.

5 In another aspect of the invention a network payment system executes payment orders. A payment order includes a sender, a beneficiary, a payment amount, and a nonce identifier. A payment order is signed by a client computer with an authenticator that is checked by the
10 payment system. Payment orders are backed by accounts in the banking system, and are authorized by the network payment system by sending messages into a financial authorization network that knows the status of these accounts. The payment system accomplishes settlement by
15 sending messages into an existing financial system network.

In another aspect, payment orders are authenticated based on the delivery address they specify. In another aspect, the payment system will specify in its
20 authorization legal delivery addresses. In another aspect, authenticators for payment orders are based on one-time transaction identifiers that are known only to the user and the payment system. In another aspect, payment orders for a given sender are only accepted from
25 certain client computer network addresses. In another aspect, the network payment system sends messages into a financial authorization system in real-time before the network payment system will authorize a payment order.

BRIEF DESCRIPTION OF THE DRAWINGS

30 Other objects, features, and advantages of the invention will appear from the following description taken together with the drawings in which:

Figure 1 is a block diagram of a typical network sales system in accordance with the invention;

- 7 -

Figure 2 is a screen snapshot of a buyer computer display of an overview page from a merchant computer;

Figure 3 is a screen snapshot of a buyer computer display of a page of digital advertisements from a
5 merchant computer;

Figure 4 is a screen snapshot of a buyer computer display of an account query page;

Figure 5 is a screen snapshot of a buyer computer display of a fulfillment page;

10 Figure 6 is a flow chart illustrating the processing of a sale between a buyer computer and a merchant computer;

Figure 7 is a flow chart illustrating the alternate processing of payment order means for obtaining
15 missing payment information;

Figure 8 is a screen snapshot of a buyer computer display of an overview page from a merchant computer that contains a query input by the user;

Figure 9 is a screen snapshot of a buyer computer
20 display of digital advertisements in response to a user's query;

Figure 10 is a screen snapshot of a buyer computer screen of a purchase confirmation;

Figure 11 is a screen snapshot of a buyer display
25 of a fulfillment page like Figure 5;

Figure 12 is a flow chart illustrating an alternate processing of a sale between a buyer computer and a merchant computer where a payment order is pre-authorized;

30 Figure 13 is a block diagram of a typical network payment system in accordance with the invention;

Figure 14 is a flow chart illustrating the authentication, authorization, and settlement of a payment order;

- 8 -

Figure 15 is a flow chart illustrating an alternate processing of the authentication and verification of a payment order where transaction identifiers are used; and

5 Figure 16 is a flow chart illustrating an alternate processing of the authorization of a payment order where real-time approval from the financial authorization network may not be obtained.

DESCRIPTION OF A PARTICULAR PREFERRED EMBODIMENT

10 A network sales system 200 as shown in Figure 1 employs a network 67 to interconnect a plurality of buyer computers 61 and 62, merchant computers 63 and 64, each merchant computer with respective digital advertisement databases 65 and 66, and a payment computer 68. A user
15 of the system employs a buyer computer to retrieve advertisements from the merchant computers, and to purchase goods of interest. A payment computer is used to authorize a purchase transaction.

20 A digital advertisement includes a product description and a price. In digital advertisement database 65 prices and descriptions may be stored separately, and one price may apply to many product descriptions.

25 In an alternate embodiment, the network sales system further includes external devices that are kept in the possession of users so that the users can authenticate themselves when they use a buyer computer.

30 The software architecture underlying the particular preferred embodiment is based upon the hypertext conventions of the World Wide Web. Appendix A describes the Hypertext Markup Language (HTML) document format used to represent digital advertisements, Appendix B describes the HTML forms fill out support in Mosaic 2.0, Appendix C is a description of the Hypertext
35 Transfer Protocol (HTTP) between buyer and merchant

- 9 -

computers, and Appendix D describes how documents are named with Uniform Resource Locators (URLs) in the network of computers. A document is defined to be any type of digital data broadly construed, such as
5 multimedia documents that include text, audio, and video, and documents that contain programs.

Figure 2 shows an overview screen that has been retrieved from a merchant computer by a buyer computer and displayed by the buyer computer. It includes links
10 1, 2, and 3 that when activated by a user cause the buyer's computer to take specified actions. In the case of link 1, the document shown in Figure 3 is retrieved from a merchant computer and displayed. In the case of link 2, a short audio segment is retrieved from a
15 merchant computer and played. In the case of link 3, the query that can be entered into the query dialog box 4 is sent to a merchant computer, and a document is retrieved from the merchant computer and displayed.

Figure 3 shows a document that contains three
20 digital advertisements. The digital advertisements have been retrieved from the merchant computer after the activation of link 3. The merchant computer may set the prices contained in the advertisements based on the on the identity of the user as determined, for example, by
25 the network address of the requesting buyer computer. The document includes links 5, 6, and 7 that are used to purchase the products described by the advertisements. For example, if link 5 is activated the missing payment information document shown in Figure 4 is retrieved from
30 the merchant computer and displayed.

Figure 4 is a missing payment information document that is used to gather user account information for the requested purchase in an HTML form. Radio
35 buttons 8, 9, 10, 11, 12 are used to select a means of payment, dialog box 13 is used to enter an account

- 10 -

number, dialog box 14 is used to enter an optional authenticator for the account, purchase button 15 is used to send the account information to the merchant computer and proceed with the purchase, link 16 is used to abort the purchase and return to the document shown in Figure 2, and dialog box 17 is used to enter optional user information that is associated with the purchase and ultimately used by a financial institution as part of a textual billing identifier for the purchase transaction. 10 If provided, this additional information is included in the payment order for the purchase.

Figure 5 is a fulfillment document 18 that is produced once valid account information is provided to the missing payment information document in Figure 4 and 15 purchase button 15 is activated.

Figure 6 is a flowchart that more fully describes the information flow in the purchase transaction shown in Figures 2 to 5. An initial user inquiry 19 from activating link 1 results in the HTTP request 20 for a specific document with a specified URL. The URL 20 specifies the name of the merchant computer. The merchant computer retrieves the document given the URL at 21, and returns it to the buyer computer at 22. The buyer computer displays the resulting HTML document at 25 23. When the user activates link 5, an HTTP request 25 is sent to the merchant computer requesting the document.

In an alternate embodiment, document 22 is executed at 23 as a program. A program is defined as a set of instructions that can exhibit conditional behavior 30 based upon user actions or the environment of the buyer computer. As is known to those skilled in the art, there are many techniques for representing programs as data. The program can be interpreted or it can be directly executed by the buyer computer. The program when 35 executed will cause the buyer computer to interact with

- 11 -

the user leading to the user purchase request 24, and the purchase message 25.

The merchant computer then attempts to construct a payment order at 26 using the information it has gathered about the user. The buyer computer may have previously supplied certain credentials using fill out forms or other account identification means such as providing the network address of the buyer computer in the normal course of communication. If the buyer computer is able to construct a complete payment order at 26 the payment order is sent to a payment computer for authorization at 27. If a payment order can be constructed, processing continues at 28.

Alternatively, the buyer computer may construct the payment order at 24 and send it to the merchant computer at 25. In this case, the payment order assembly steps at 26, at the merchant computer, may only need to forward the payment order from the buyer computer.

A payment order includes user account information, merchant account information, an amount, and a nonce identifier that has not been previously used for the same user account. Variations of payment orders can be constructed, including payment orders that specify user or merchant identifiers in place of account information, payment orders that specify a valid time period, payment orders that specify foreign currencies, and payment orders that include comment strings. Part of the process of constructing a payment order is creating a corresponding authenticator using one of the authenticator methods described below.

In the illustrated embodiment of Figures 3 and 4, the merchant computer does not have sufficient information to construct a payment order at 26 and thus at 33 (Figure 7) constructs and returns a missing payment information document in response to request 25.

- 12 -

Operation 33 includes in the constructed document appropriate form fields based on what information the merchant computer has already collected from the user. The document is returned to the buyer computer at 34 and is displayed at 35. When the user presses the purchase button 15, the contents of the form are transmitted to the merchant computer, at 36, to a specific URL name, using an HTTP request. Based on the supplied form fields, the merchant computer constructs a complete payment order. Alternatively, the buyer computer may construct the payment order at 35 and send it to the merchant computer as part of step 36. In this case, the payment order assembly steps 37 at the merchant computer simply passes on the payment order from the buyer computer. The payment order is sent to the payment computer in a message at 38.

In either case, the flowchart continues in Figure 6 where the payment computer checks the authorization of the payment order at 28. If the payment system authorizes the request, an authorization message at 29 is returned to the buyer computer, and the merchant computer checks at 30 that the authorization message came from the payment computer using the authenticator mechanism described below. Assuming that the authorization message is valid, the merchant computer performs fulfillment at 30, returning the purchased product in response at 31. In our example in Figure 5 the response at 31 is document 18 that was the logical target of link 5. If the payment system does not authorize the payment order then response 31 is a rejection of the user's purchase request.

In an alternate embodiment, step 30 can encrypt the document using a key that is known to the buyer computer. As is known to those skilled in the art, the key can be communicated to the merchant computer using convention key distribution protocols. In this manner

- 13 -

the document will be protected from disclosure to other users.

The fulfillment step at 30 can alternatively schedule a physical product to be shipped via ordinary
5 mail or other means. This can be accomplished by updating a fulfillment request database or by sending a message to a shipping system. In this case the response at 31 is a confirmation that the product has been scheduled to ship. In this way the network sales system
10 can implement an electronic mail order system.

Figures 8, 9, 10, and 11 show a second example that uses query based access to digital advertisements. It is assumed that the previous example was used by the user immediately before at the same buyer computer.

15 Figure 8 shows the overview screen where the query "movie review" has been entered into dialog box 39. When the user activates process button 40, the merchant searches databases as described by the URL attached to button 40, and creates a response document as shown in
20 Figure 9.

Figure 9 shows digital advertisements 39, 40, 41, 42, 43, and 44 that were found in response to the query initiated by button 40. A scroll bar 45 shows that there are additional digital advertisements that are not shown.
25 When link 46 is activated, the missing account information document shown in Figure 10 is returned by the merchant computer.

Figure 10 shows that the merchant computer has partial information on the buyer's account. Message 47
30 shows that the merchant computer already knows the buyer's account number. Purchase button 48 will send the optional user reference string in dialog box 50 to the merchant computer described by the URL behind button 48 and purchase the product corresponding to digital

- 14 -

advertisement 39. Cancel link 49 will return the user to the document shown in Figure 2.

When purchase button 48 is activated, a document 51 is sent by the merchant computer and displayed by the
5 buyer computer as shown in Figure 11.

Figure 12 shows an alternative method of processing a sales transaction. In this method when the user requests a purchase at 52, the buyer computer constructs a payment order at 53 and sends it for
10 approval to the payment computer at 54. The payment computer authorizes the payment order at 55; and when the payment order is authorized, returns an unforgeable certificate at 56 that the payment order is valid. Means
of creating such unforgeable certificates are described in
15 authenticator method number one below. If at step 55 the payment order is not authorized, a rejection message is sent at 56 and the sales transaction is terminated.

The buyer computer then proceeds at 57 to send a pre-authorized purchase request to the merchant computer.
20 The unforgeable certificate 56 is included in a purchase message at 57 that is sent at 58 to the merchant computer. Based upon the pre-authorized payment order the merchant computer performs fulfillment at 59 and returns the product at 60. In a variation, the merchant
25 computer at 59 checks to ensure the payment order has not been previously used. This can be accomplished by checking with a payment computer or maintaining a merchant computer database of previously accepted payment orders. The unforgeable certificate created at step 56
30 does not need to include the user account information. This variation is useful if the user wishes to make purchases and remain anonymous to the merchant.

- 15 -

A Network Payment System

A network payment system 300 as shown in Figure 13, employs a public packet-switched network 69 to interconnect a plurality of client computers 70 and 71, and a plurality of payment computers such as 72, each payment computer having an account database 73, a settlement database 74, an authorized address database 75, a sender credential database 76, a financial system interface 77, and a real-time authorization interface 78. The interfaces 77 and 78 may be implemented by a single communications line.

In an alternate embodiment, the network payment system further includes external devices that are kept in the possession of users so that the users can authenticate themselves when they use a buyer computer.

Account database 73 maintains temporal spending amounts, such as the amount spent in the current day, and also maintains temporal spending limits. The account database may also maintain a translation between principal identifiers and external account identifiers. Settlement database 74 records committed payment orders along with any authorization information for the orders that was obtained from interface 78. Address database 75 maintains for each sender a list of authorized buyer computer and delivery addresses. Credential database 76 maintains a list of credentials for principals and information that can be used to authenticate principals.

Figure 14 is a flowchart that describes the operation of the payment system. A client computer 71 constructs a payment order at 79, and computes and adds an authenticator to the payment order at 80. The payment order is sent at 81 to a payment computer, where the authenticator is verified at 82 to ensure that the payment order was originated by the sender it describes.

- 16 -

Below we present different means of implementing 80 and 82.

If the payment order is authentic and address restrictions are desired, at 83, either or both of the client computer address or the specified delivery address can be checked against address database 75. If address restrictions are desired and if the addresses in the payment order are not in the database, the payment computer sends a rejection message to the client computer. Address database 75 specifies, for each principal, acceptable client computer addresses and delivery addresses. A delivery address can be a network address, or a street address for packaged goods. As is known in the art, database 75 can include wild-card specifications and similar techniques to reduce its size.

For example, database 75 could contain an entry for principal identifier "*@acme.com" restricting legal delivery addresses to "computer: *.com", "computer: cmu.edu", and "surface: *, 34 Main Street, Anytown, USA", indicating that any user at the company Acme can order products to be delivered to the network address at Acme or the university CMU, or to anyone at 34 Main Street, Anytown, USA.

If payment order address restrictions are not desired or have been checked, processing continues at 84 where the payment order is checked for replay and temporal spending limits. Replay is checked for by making sure that the sender did not previously present a payment order with the same nonce by checking an index of committed payment orders by nonce in settlement database 74. If nonces are based on time, then a payment order that is older than an administratively determined value can be rejected out of hand. Time based nonces or sequential nonces permit old nonces to be removed from the settlement database 74. If a payment order has been

- 17 -

previously processed or its nonce is too old, the payment order computer sends a rejection message to the client.

After the payment order passes the replay check, temporal spending limits are checked in account database 73. These spending limits can be applied on a per sender, per group of senders, and per payment system basis to limit fraud risk. The limits can be applied to any duration of time, for example a maximum spending amount per hour or per day. If the payment order would violate a spending limit, the payment computer sends a rejection message to the client.

Once the payment order passes the temporal spending check at 84, a message is constructed at 85 to check that the external account that backs the sender's payment system account has adequate funds or credit. If the sender identifier in the payment order is not already an account number in the external financial system, it is translated into a corresponding account number in the external financial system using account database 73. A real-time authorization request message is sent at 86 to the external financial system over interface 78. If the external financial system approves authorization request 86, an authorization message is returned at 87. If request 86 is not approved, the payment computer sends a rejection message to the client at 87.

In a variation of the above described approach, processing continues at 95 after 84. At 95 real-time authorization is only obtained when the total of a sender's payments since the last real-time authorization reaches a preset value, or the payment order is over a preset amount. These preset values can be optionally recorded on a per principal basis in database 73 or can be administratively determined for all principals. In this manner, the number of messages to the external financial system can be reduced. In addition, the

- 18 -

payment system can avoid making real-time authorization requests for small payments when the risk is acceptable to the payment system operator. If real-time authorization is necessary, processing continues at 85
5 after 95. If real-time authorization is not necessary for a request, at 100 the payment order amount is added to the sender's total of payments since the last real-time authorization in database 73, and processing continues at 88.

10 In another variation after 100 a check is made at 101 in database 73 to see if a background authorization process should be scheduled. A background authorization process permits the payment computer to continue its normal processing while it checks with the financial
15 authorization network on the sender's account. This mechanism can be used to limit payment system risk. If the background authorization fails, the account is suspended by so updating database 73. If the sender's total of payments since last authorization is over a
20 preset value stored in 73 then a background authorization process is scheduled at 102. Otherwise processing continues at 88.

In another variation, at 95 and 101 authorizations are obtained based on the amount spent
25 since last authorization and time since last authorization.

At 88 the payment order is committed to execution and is recorded in settlement database 74. Recorded with the payment order in database 74 are portions of
30 authentication message 87 that show that the payment computer contacted the remote financial system. The amount of the payment order is added to running temporal spending records in database 73, and an authorization message is sent to the client computer at 90. The
35 authorization message includes the payment order. In an

- 19 -

alternate embodiment, at 90 the authorization message contains a truncated payment order that includes at least the payment order's sender and the payment order's unique nonce.

5 In an alternate embodiment, the authorization message sent to the client at 90 includes at least one legal delivery addresses for the sender as determined from database 75.

10 Authorization message 90 must be transmitted in such a way that the client computer can be sure that it came from the payment computer. At 89 a payment system specific authenticator is added payment order. At 91 this authenticator is checked by the client computer. The steps at 89 are a dual of step 80, and the steps at
15 91 are a dual of step 82. The authentication means for steps 89 and 91 are described below.

 Finally, settlement is performed at 92 in the external financial system 77 between external accounts that correspond to the sender and the beneficiary. If
20 settlement is accomplished as part of real-time authorization at steps 86 and 87, as may occur in a real-time debit network, then no other steps need to be taken. If settlement is not accomplished as part of the authorization process, then financial system messages are
25 sent to interface 77 to effect settlement. Depending on the external accounts involved, these messages may include electronic funds transfer messages or automated clearinghouse messages.

 In an alternate embodiment, at 92 settlement
30 messages are sent to reconcile net transfer balances between principles on a temporal basis, for example once a day. In this embodiment the number of settlement messages can be less than the number of payment orders.

 Authenticators may be created and checked using
35 one of the following methods. The payment computer can

- 20 -

use any of the first four methods, and the client computer can use any of the methods described.

In a first method for authenticators, at steps 80 or 89, a digest of the payment order is signed by the sending computer using a public-key cryptographic system such as RSA. This signature is used as the authenticator. As is well known in the art, the signing can be accomplished using a private key created from a public-key pair, where the signing key is only known by the signer, and the other public key is known to the receiving computer. At the payment computer the public key corresponding to each sender is kept in credential database 76. The private key for the payment service is also kept in database 76. At steps 82 or 91, the signature of the received message is checked using the public key known to the receiving computer.

In a second method for authenticators, at steps 80 or 89, a digest of the payment order is signed by the sending computer with a private key cryptosystem such as DES. This signature is used as the authenticator. At the payment computer, the private key corresponding to each sender is kept in credential database 76. At step 80, a digest of the payment order is signed by the client computer, and at step 89 a digest of the payment order with an added approval code is signed by the payment computer using the same private key. At steps 82 or 91, the signature of the received message is checked using the shared private key.

In a third method for authenticators, at step 80 the authenticator is computed by a protected device external to the system such as a Smart-Card. A protected device is specifically designed to be extremely difficult both to replicate and to compromise. In this method, the payment order is communicated at 80 to a Smart-Card. The Smart-Card computes and signs a digest of the payment

- 21 -

order, and then communicates the signature back at 80 to be used as an authenticator. A Smart-Card produced authenticator uniquely associates a payment order with its creating Smart-Card. This is accomplished by having
5 the Smart-Card contain a secret key "K" that is used to create a digital signature of the payment order. "K" is never released outside of the Smart-card. The Smart-Card is designed to make it computationally infeasible to compute "K" even with possession of the device. In this
10 method, at step 82, a signature checking key from database 76 is used to check the authenticator. In an alternate embodiment, a user must manually signal their acceptance of each payment order on an input device that is part of the external device before the authenticator
15 is created by the external device.

In a fourth method for authenticators, at steps 80 or 89, a network address is used as an authenticator. At steps 82 or 91, a digest of the payment order is sent back to the specified network address along with a random
20 password. The computer at the specified network address must then return the payment order digest along with the password. If the network guarantees to deliver messages to the proper network address, this method will guarantee that the user or computer at the specified network
25 address approves of the payment order. Assuming that network delivery is trusted, this method can be used to authenticate a sender computer's network address in a payment order. Alternatively, electronic mail can be used to send such confirmation messages between a user
30 and the payment system.

In a fifth method for authenticators, at step 80, the authenticator is produced by an external device that produces a sequence of non-predicable transaction identifiers that are device specific. The authenticator
35 is entered by the user into the client computer by

- 22 -

reading its display. One such device is described in U.S. Patent 4,856,062. According to this method, at step 91, the authenticator can be checked using the sender specific fixed code of the device which is kept in database 76. This sequence of steps is also shown in Figure 15 at steps 93 and 94.

In a sixth method for authenticators, at step 80, the authenticator is obtained by querying the user for a transaction identifier that is the next string from a physical list of one-time authorization strings. Such as list could be produced on a card, and the user can cross off authorization strings as they are used. According to this method, at step 91, the authenticator is checked against the next expected string from the sender using database 76. Database 76 can hold for each sender a list of random authorization strings, or can hold a sender specific secret key that was used to generate the list of authentication strings along with how many strings have been used so far. This sequence of steps is also shown in Figure 15 at 93 and 94.

In a seventh method for authenticators, at step 80 the authenticator is a previously obtained personal identification number (PIN) for the user. In this method in 91 the authenticator is checked against the expected PIN for the sender using database 76.

As will be obvious to one skilled in the art, any of the methods for creating authenticators can be used together to increase system security. For example, authenticator method six can be used to create an authenticator based on a transaction identifier, and then a payment order including a transaction identifier can be given a further authenticator using authenticator method one. In this example the resulting authenticators would be checked with their respective methods.

- 23 -

A digest of a payment order can be created with an algorithm such as MD5 [R. Rivest, The MD5 Message-Digest Algorithm, MIT Laboratory for Computer Science, Network Working Group Request for Comments 1321].

- 5 Alternatively, a digest can be the entire payment order or other functions of the payment order's component parts.

- In addition in both the sales and payment systems alternate authenticator techniques can be used such as
- 10 those described by Voydock and Kent in "Security Mechanisms in High-level Network Protocols", Computing Surveys Vol. 15, No. 2, June 1983. As will be appreciated by those skilled in the art, two-way authenticated byte-stream or remote procedure call
- 15 interface connections that protect against replay can replace our message based authenticators.

- Additions, subtractions, deletions, and other modifications of the described embodiment will be apparent to those practiced in the art and are within the
- 20 scope of the following claims.

- 24 -

CLAIMS

1. A network sales system comprising
a plurality of buyer computers and at least one
merchant computer interconnected by a communications
network,

5 means at each merchant computer for maintaining
and providing a database of digital advertisements
comprising

means for storing said digital advertisements,
each digital advertisement including a product abstract,

10 means for communicating a digital advertisement
to a buyer computer over said network in response to a
network request from said buyer computer,

means at each buyer computer for requesting,
displaying, and responding to digital advertisements

15 comprising

means responsive to a user inquiry for selecting
a merchant computer and obtaining a digital advertisement
for a product from said database of advertisements at
said merchant computer,

20 display means for displaying said advertisement,
purchase means responsive to a user request for
communicating a purchase message to said merchant
computer,

account identification means for transmitting the
25 user's account information to said merchant computer,

means, at said merchant computer, comprising
authorization means to authorize said purchase
message by sending messages into a financial system
network,

30 fulfillment means to send said product to user
conditional on approval of said authorization means.

- 25 -

2. The network sales system of claim 1 further wherein said authorization means at said merchant computer comprises

means for communicating a missing payment
5 information request message to said buyer computer to obtain missing payment information,
means for receiving said missing payment information from said buyer computer,
means for authorizing said purchase message by
10 sending messages into a financial system network,
and said account identification means at said buyer computer comprises
means responsive to said missing payment information request message to query the user for
15 additional payment information,
means to send said additional payment information to said merchant computer.

3. The network sales system of claim 1 further wherein said account identification means comprises
20 means for assembling a payment order,
means for sending said payment order to a network payment system for authorization,
and wherein said authorization means comprises
means for verifying that said payment order has
25 been previously authorized by said payment system.

4. An electronic sales system comprising
means for storing a database of digital
advertisements, each digital advertisement for a product including a program,
30 means for communicating a digital advertisement to a buyer computer,
means at said buyer computer for displaying and responding to said digital advertisement comprising

- 26 -

display means for displaying said digital advertisement by executing a portion of said advertisement as a program and performing actions as specified by said program,

5 purchase means responsive to a user request for communicating a purchase message to a merchant computer, means, at said merchant computer, comprising fulfillment means to send said product to user.

5. A network payment system comprising
10 a plurality of client computers and at least one payment computer interconnected by a public packet switched communications network,
means at a client computer for performing payment comprising

15 payment specification means for constructing a payment order from a sender to a beneficiary,

signing means for authenticating said payment order as originating from said sender,
20 means for sending said payment order to a payment computer,

means for receiving a payment order authorization message from said payment computer,

means responsive to a payment order message at
25 said payment computer comprising

verification means for verifying that said sender originated said payment order,
authorization means for sending a message into a financial authorization network to verify that said
30 sender has adequate funds or credit and receiving an authorization in response,

means for recording said payment order and authorization in a settlement database,

- 27 -

response means for sending an authorization message to said client computer,
means for sending at least one message into a financial system network to transfer funds from
5 said sender to said beneficiary.

6. The network payment system of claim 5 further wherein said payment specification means comprises
means for constructing a payment order, said payment order including a delivery address,
10 and said verification means comprises
means for verifying that said sender originated said payment order and checking said delivery address against a database of allowed delivery addresses for said sender.

15 7. The network payment system of claim 5 further wherein said response means comprises
means for determining allowed delivery addresses for said sender,
means for sending an authorization message to
20 said client computer that includes allowed delivery addresses.

8. The network payment system of claim 5 further wherein said signing means comprises
means for generating the next expected
25 transaction identifier for said sender and using it to create an authenticator,
and wherein said verification means comprises
means for generating the next expected transaction identifier for said sender, and
30 means for verifying that said authenticator was created using said transaction identifier.

- 28 -

9. The network payment system of claim 5 further wherein said signing means comprises means for generating an authenticator using an external device,
5 and wherein said verification means comprises means for verifying that said authenticator was created using said external device.

10. The network payment system of claim 5 further wherein said payment specification means
10 comprises means for constructing a payment order from a sender, said payment order including a client computer's network address,
and said verification means comprises
15 means for verifying said payment order was constructed at said client computer's network address and checking said client address against a database of allowed client addresses for said sender.

11. The network payment system of claim 5
20 further wherein said authorization means comprises determination means for determining the necessity for real-time authorization,
means for performing real-time authorization conditioned on said determination means.

25 12. A method for effecting sales over a network sales system having a plurality of buyer computers and at least one merchant computer interconnected by a communications network, encompassing the steps of
maintaining and providing a database of digital
30 advertisements at each merchant computer
storing said digital advertisements, each digital advertisement including a product abstract,

- 29 -

communicating a digital advertisement to a buyer computer over said network in response to a network request from said buyer computer,

requesting, displaying, and responding at each
5 buyer computer to digital advertisements comprising the steps of

selecting in response to a user inquiry a merchant computer and obtaining a digital advertisement for a product from said database of advertisements at
10 said merchant computer,

displaying said advertisement,

communicating in response to a user request a purchase message to said merchant computer,

transmitting the user's account information to
15 said merchant computer,

authorizing at said merchant computer said purchase message by sending messages into a financial system network, and

sending said product to said user conditional on
20 approval from said authorizing step.

13. The network sales method of claim 12 further wherein said authorizing step, at said merchant computer, comprises the steps of

communicating a missing payment information
25 request message to said buyer computer to obtain missing payment information,

receiving said missing payment information from said buyer computer,

authorizing said purchase message by sending
30 messages into a financial system network,

and said account identification step at said buyer computer comprising the steps of

- 30 -

querying the user for additional payment
information responsive to said missing payment
information request message,
and sending said additional payment information
5 to said merchant computer.

14. The network sales method of claim 12 further
wherein said account identification step comprises the
steps of
assembling a payment order, and
10 sending said payment order to a network payment
system for authorization,
and wherein said authorization step comprises the
step of
verifying that said payment order has been
15 previously authorized by said payment system.

15. An electronic sales method comprising the
steps of
storing a database of digital advertisements,
each digital advertisement for a product including a
20 program,
communicating a digital advertisement to a buyer
computer,
displaying and responding to said digital
advertisement at said buyer computer comprising the steps
25 of
displaying said digital advertisement by
executing a portion of said advertisement as a program
and performing actions as specified by said program,
communicating a purchase message in response to a user
30 request to a merchant computer,
sending at said merchant computer said product to
user.

- 31 -

16. A network payment method comprising the steps of interconnecting a plurality of client computers and at least one payment computer by a public packet switched communications network,

5 performing payment at a client computer comprising the steps of

constructing a payment order from a sender to a beneficiary,

10 authenticating said payment order as originating from said sender,

sending said payment order to a payment computer, and receiving a payment order authorization message from said payment computer,

15 responding to a payment order message at said payment computer comprising the steps of

verifying that said sender originated said payment order,

sending a message into a financial authorization network to verify that said sender has adequate funds or

20 credit and receiving an authorization in response,

recording said payment order and authorization in a settlement database,

sending an authorization message to said client computer,

25 and sending at least one message into a financial system network to transfer funds from said sender to said beneficiary.

17. The network payment system of claim 16 further wherein said constructing step means comprises

30 the steps of

constructing a payment order, said payment order including a delivery address,

and said verifying step comprises the steps of

- 32 -

verifying that said sender originated said payment order, and
checking said delivery address against a database of allowed delivery addresses for said sender.

5 18. The network payment method of claim 16 further wherein said second sending step comprises the steps of
 determining allowed delivery addresses for said sender,
10 and sending an authorization message to said client computer that includes allowed delivery addresses.

 19. The network payment method of claim 16 further wherein said authenticating step comprises the
15 steps of
 generating the next expected transaction identifier for said sender and using it to create an authenticator,
 and wherein said verifying step comprises the
20 steps of
 generating the next expected transaction identifier for said sender,
 and verifying that said authenticator was created using said transaction identifier.

25 20. The network payment method of claim 16 further wherein said authentication step comprises the step of
 generating an authenticator using an external device,
30 and wherein said verifying step comprises the steps of

- 33 -

verifying that said authenticator was created using said external device.

21. The network payment method of claim 16 further wherein said constructing step comprises the step
5 of

constructing a payment order from a sender, said payment order including a client computer's network address,

and said verifying step means comprises the steps
10 of

verifying said payment order was constructed at said client computer's network address,

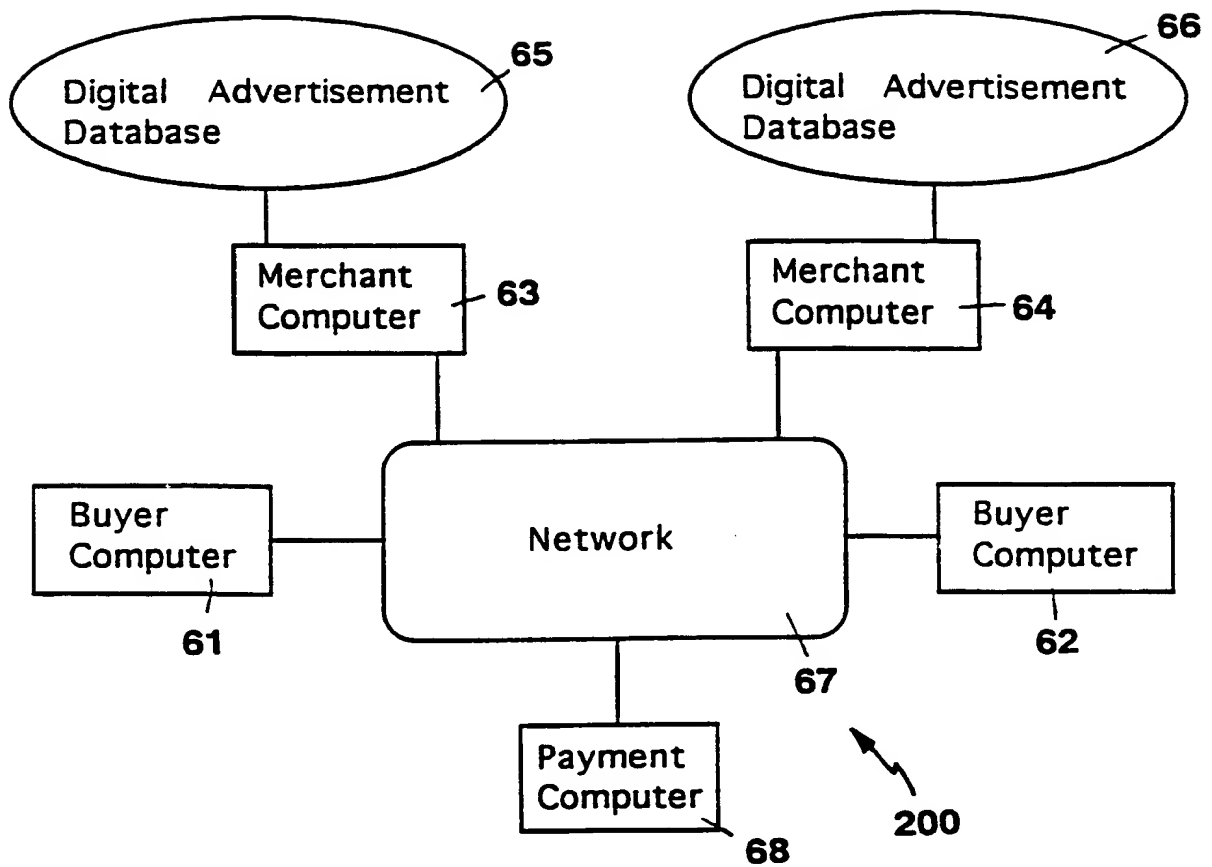
and checking said client address against a database of allowed client addresses for said sender.

22. The network payment method of claim 16 further wherein said second sending step comprises the steps of

determining the necessity for real-time authorization,

20 and performing real-time authorization conditioned on its determined necessity.

1/16

**FIG. 1**

2/16

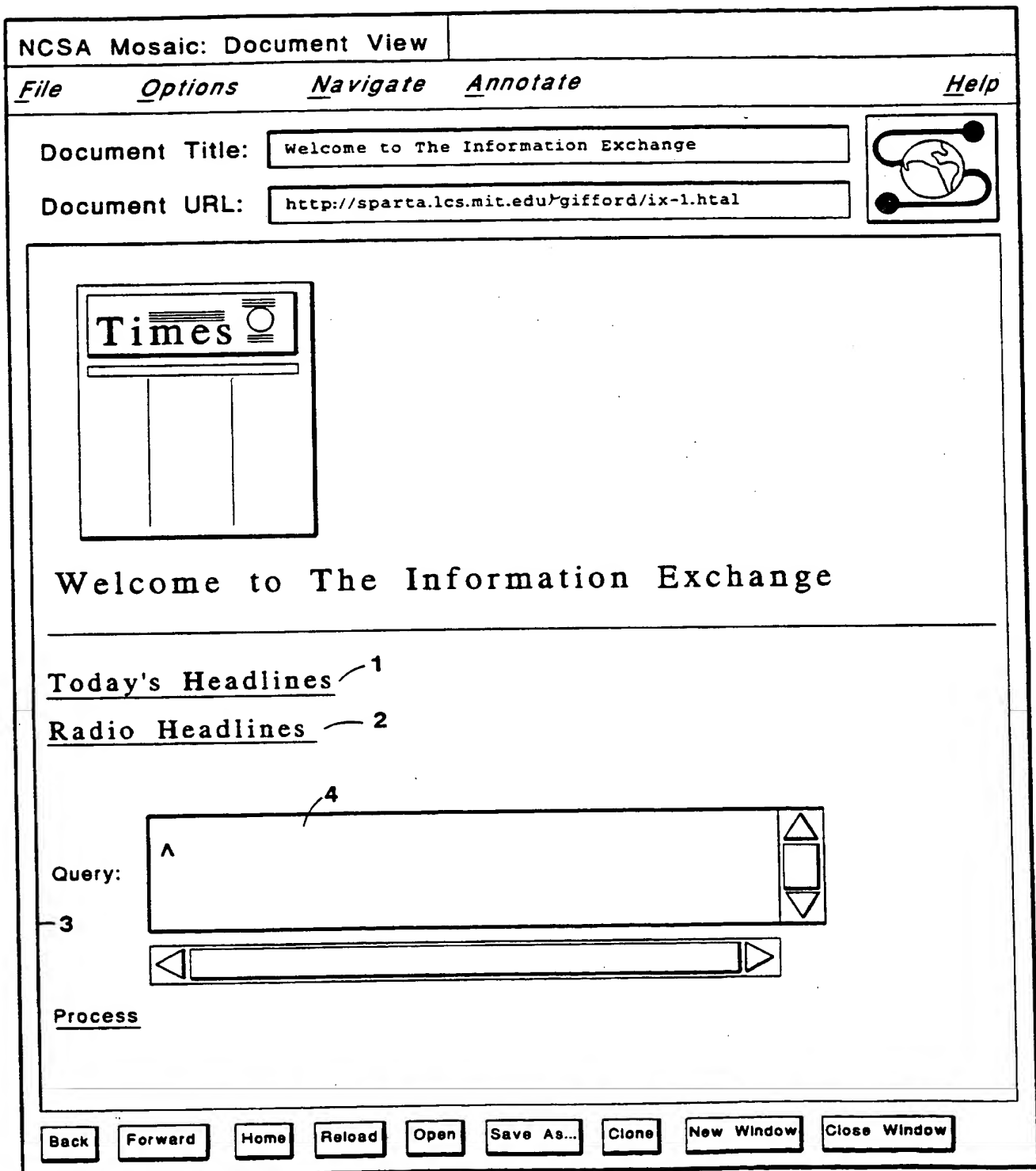


FIG. 2

3/16

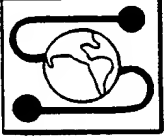
NCSA Mosaic: Document View		
<u>F</u> ile	<u>O</u> ptions	<u>N</u> avigate
<u>A</u> nnotate		<u>H</u> elp
Document Title:	The Information Exchange eadlines	
Document URL:	http://sparta.lcs.mit.edu/gifford/ix-2.htal	
<h2 style="text-align: center;">New York Times Headlines</h2> <hr/> <div style="padding: 10px;"> <p>SHUTTLE HUBBLE (Houston)- Arriving for a house call 357 miles above Earth, the astronauts of the space shuttle Endeavor on Saturday reached out with a mechanical grappling arm and easily snared the Hubble space telescope and prepared to treat the crippled spacecraft in five days of the most complex orbital repairs yet attempted. By John Noble Wilford</p> <p style="text-align: right;"><u>5</u></p> </div> <hr/> <div style="padding: 10px;"> <p>HEALTH-ALLIANCE (Washington)- If the Clinton health plan becomes law, ti will put a new institution into the lives of most Americans: the health alliance. Almost no other aspect of the plan is so little understood or so radically different from the status quo. By Robin Toner.</p> <p style="text-align: right;"><u>6</u></p> </div> <hr/> <div style="padding: 10px;"> <p>GAMBLING (Las Vegas)- The newest perspective on the booming national industry of legalized gambling is now open for business: futuristic virtual-reality rides to soothe the losers' souls, just up the theme park escalator from acres of the latest video slot machines. By Francis X. Clines.</p> <p style="text-align: right;"><u>7</u></p> </div> <hr/>		
<div style="display: flex; justify-content: space-between;"> Back Forward Home Reload Open Save As... Clone New Window Close Window </div>		

FIG. 3

4/16

NCSA Mosaic: Document View

File Options Navigate Annotate Help

Document Title:

Document URL:

Digital Copyright License Purchase

In exchange for the specified fee you will be licensed for individual use use of copyrighted material.

Charge \$1.00 to my:

1. ☐ Intetet Card — 8
2. ☐ Mastercard — 9
3. ☐ Visa — 10
4. ☐ American Express — 11
5. ☐ Discover — 12

Account Number: — 13

Authenticator: — 14

Purchase — 15

Cancel — 16

Your Reference: 17

FIG. 4

5/16

18

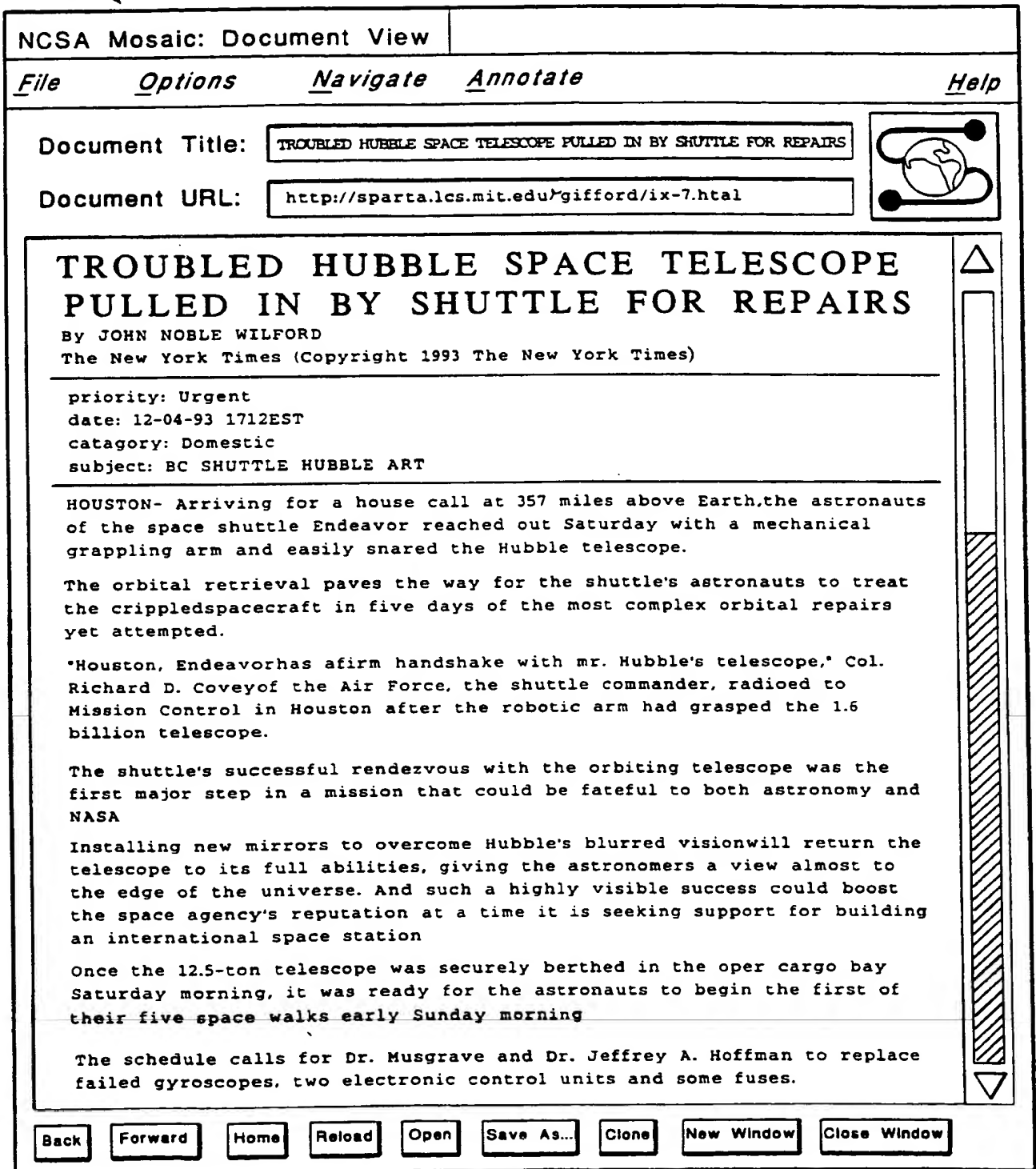


FIG. 5

6/16

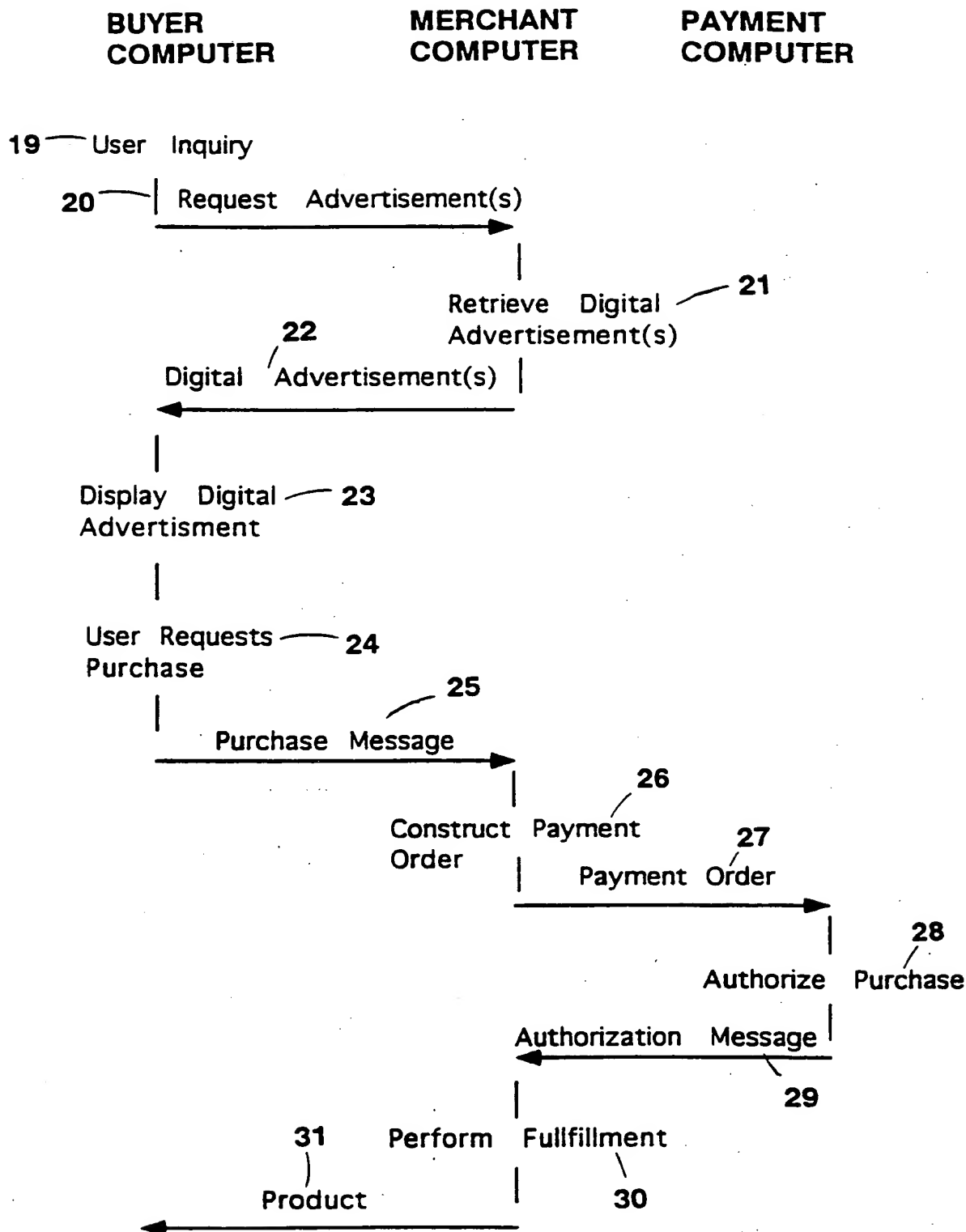
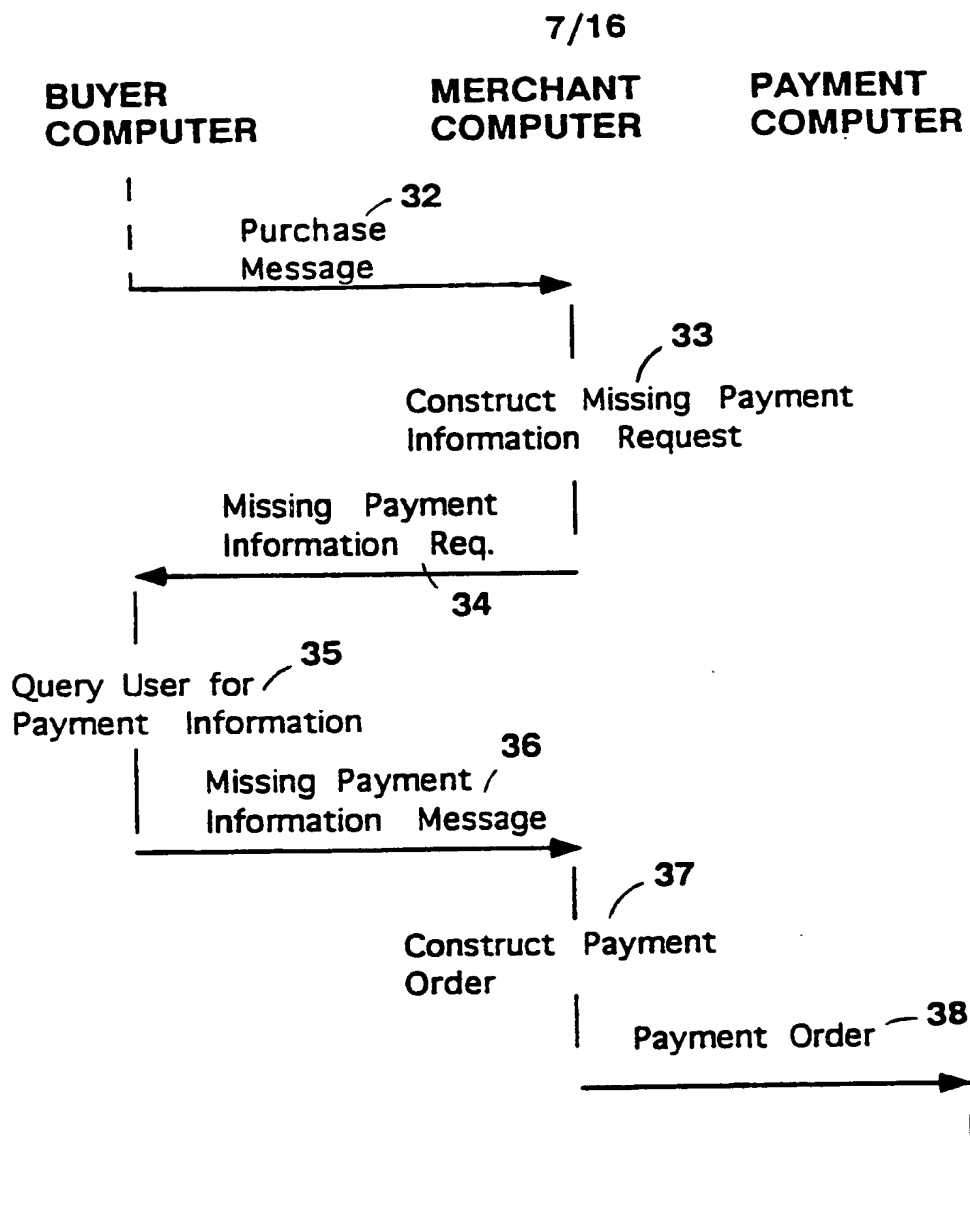


FIG. 6

**FIG. 7**

8/16

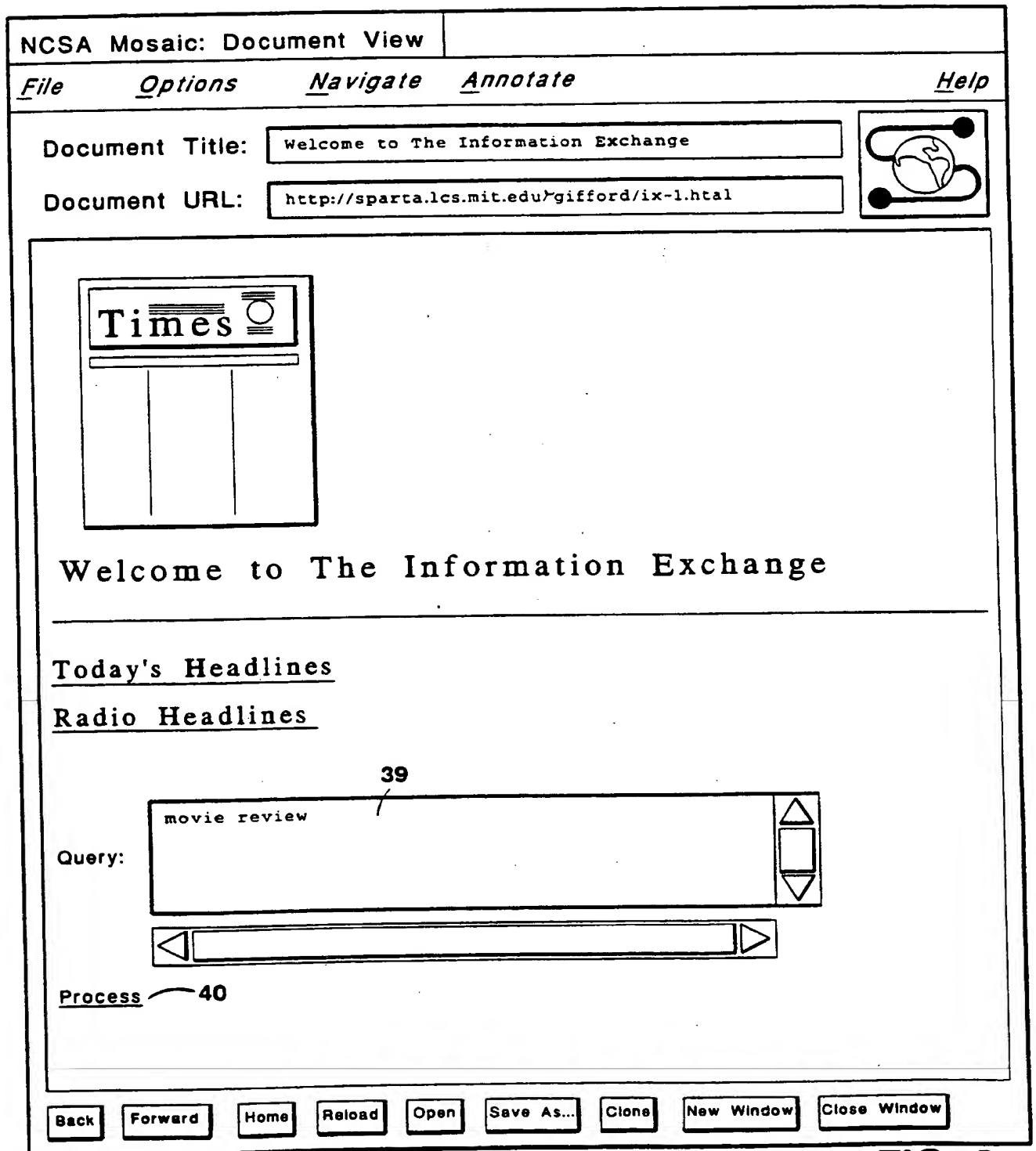


FIG. 8

9/16

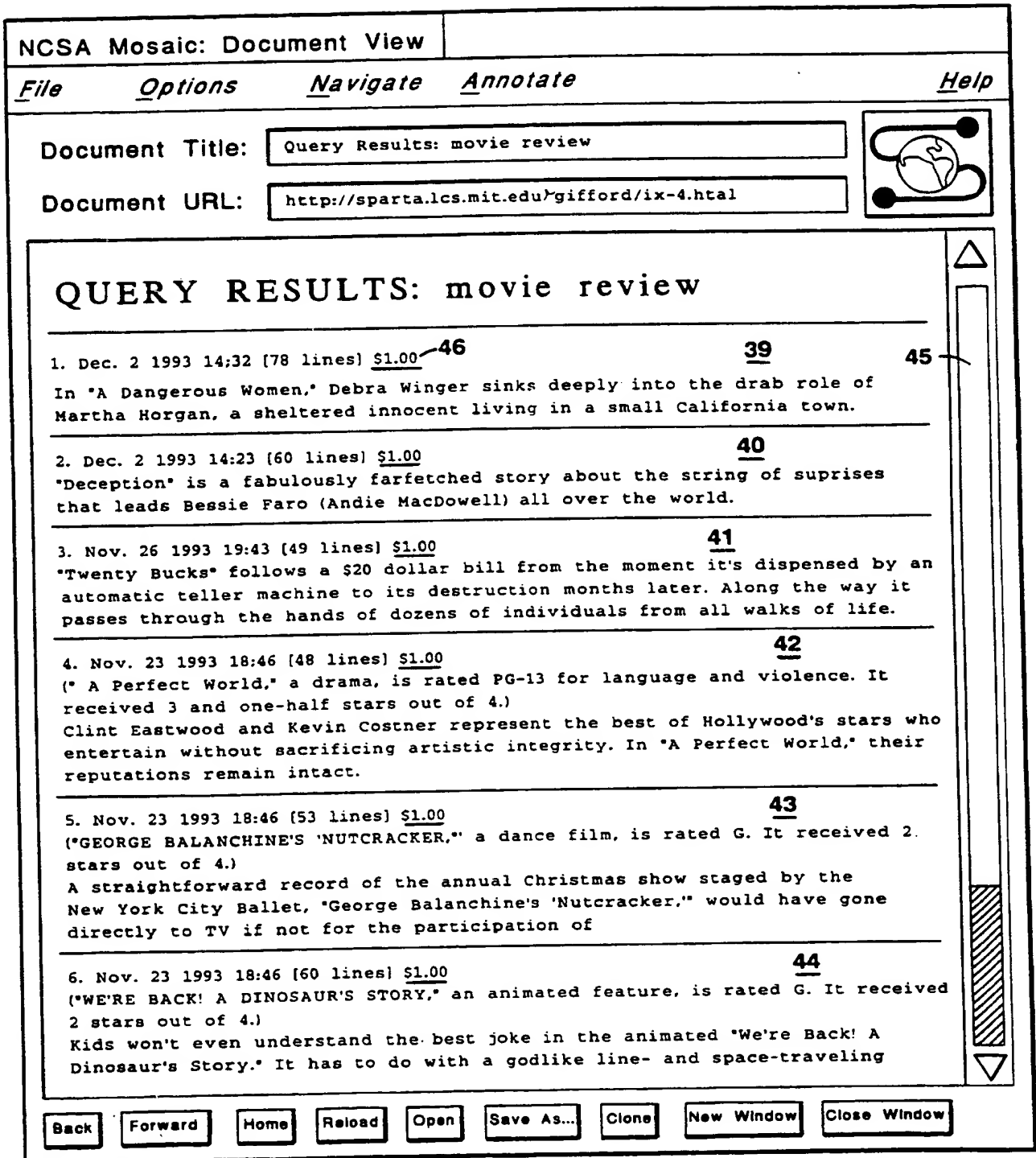


FIG. 9


10/16

NCSA Mosaic: Document View

File Options Navigate Annotate Help

Document Title:

Document URL:



Digital Copyright License Purchase

In exchange for the specified fee you will be licensed for individual use of the copyrighted material


Confirm a charge of \$1.00 ov your VISA 4262 1501 2000 1466 —⁴⁷


Purchase —⁴⁸

Cancel —⁴⁹

Your Reference:

50





Back Forward Home Reload Open Save As... Clone New Window Close Window

FIG. 10

11/16

51

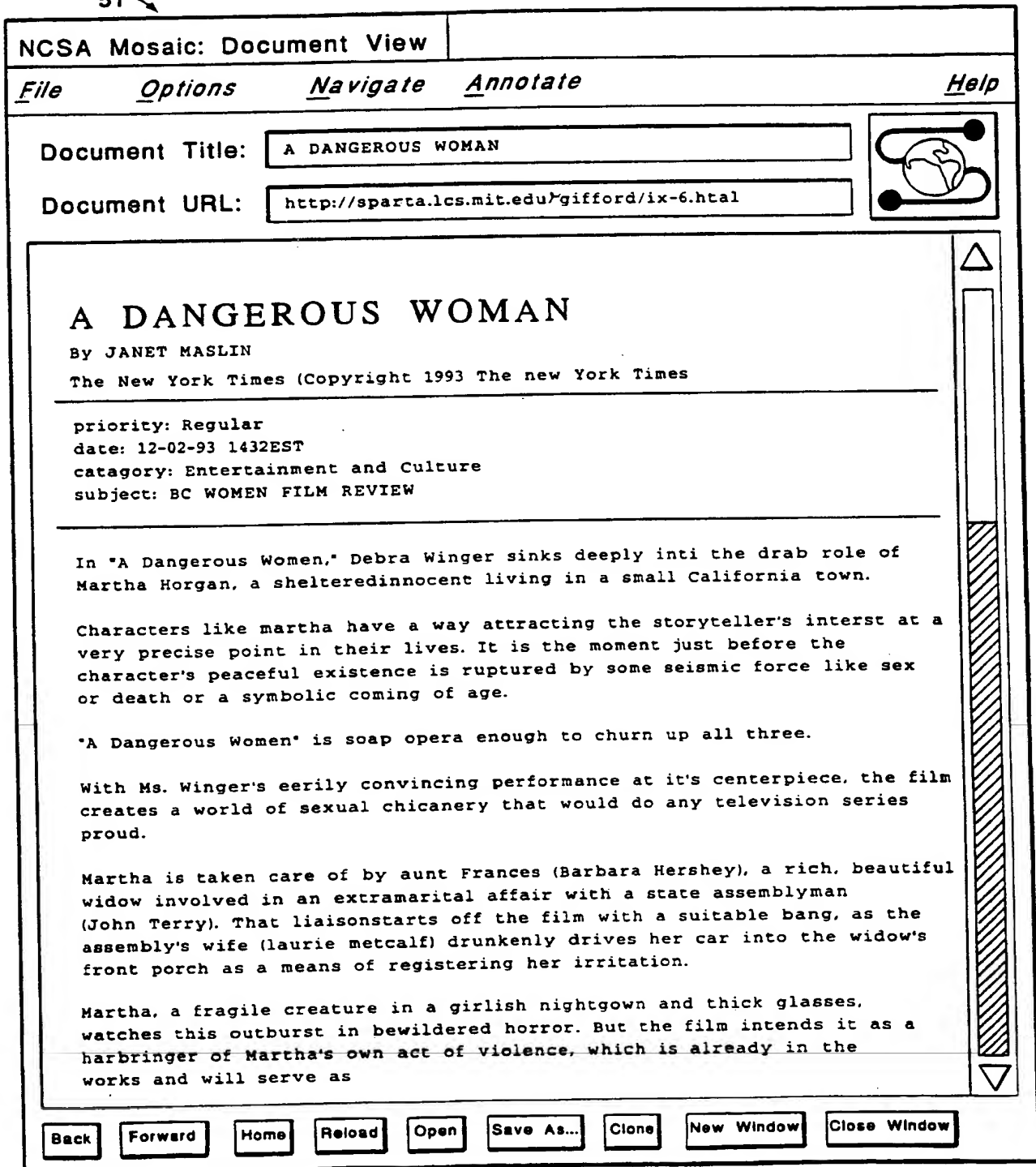


FIG. 11

12/16

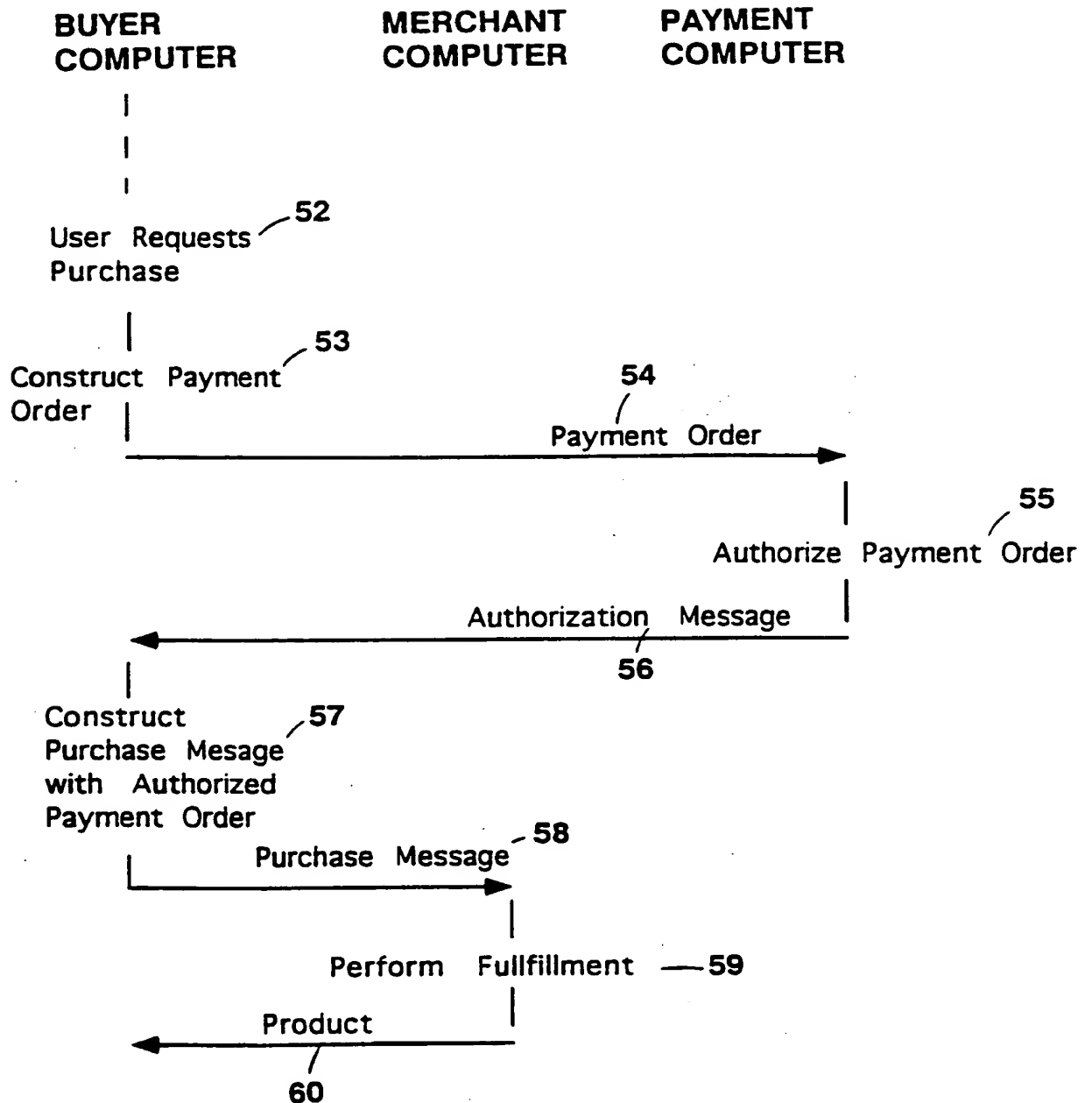
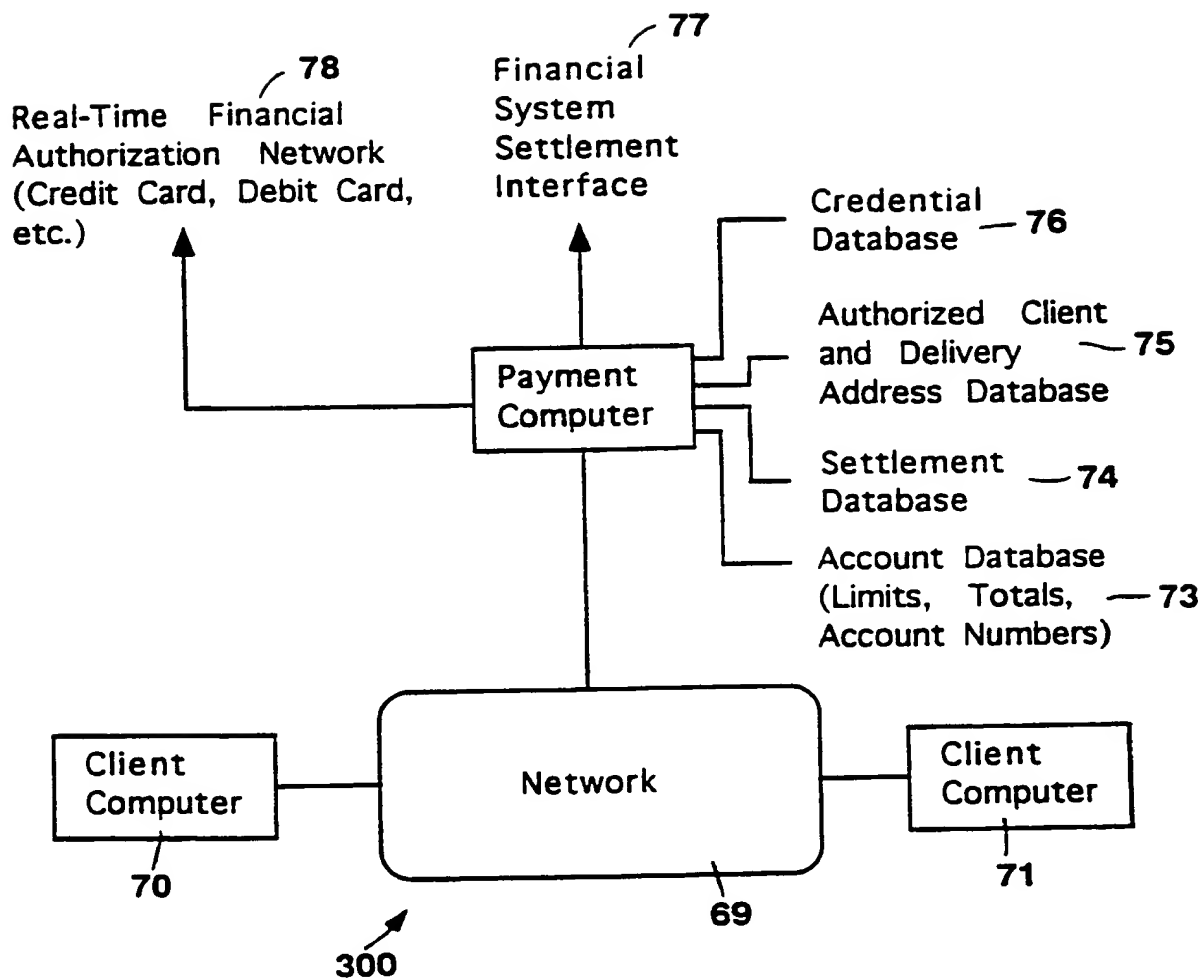


FIG. 12

13/16

**FIG. 13**

14/16

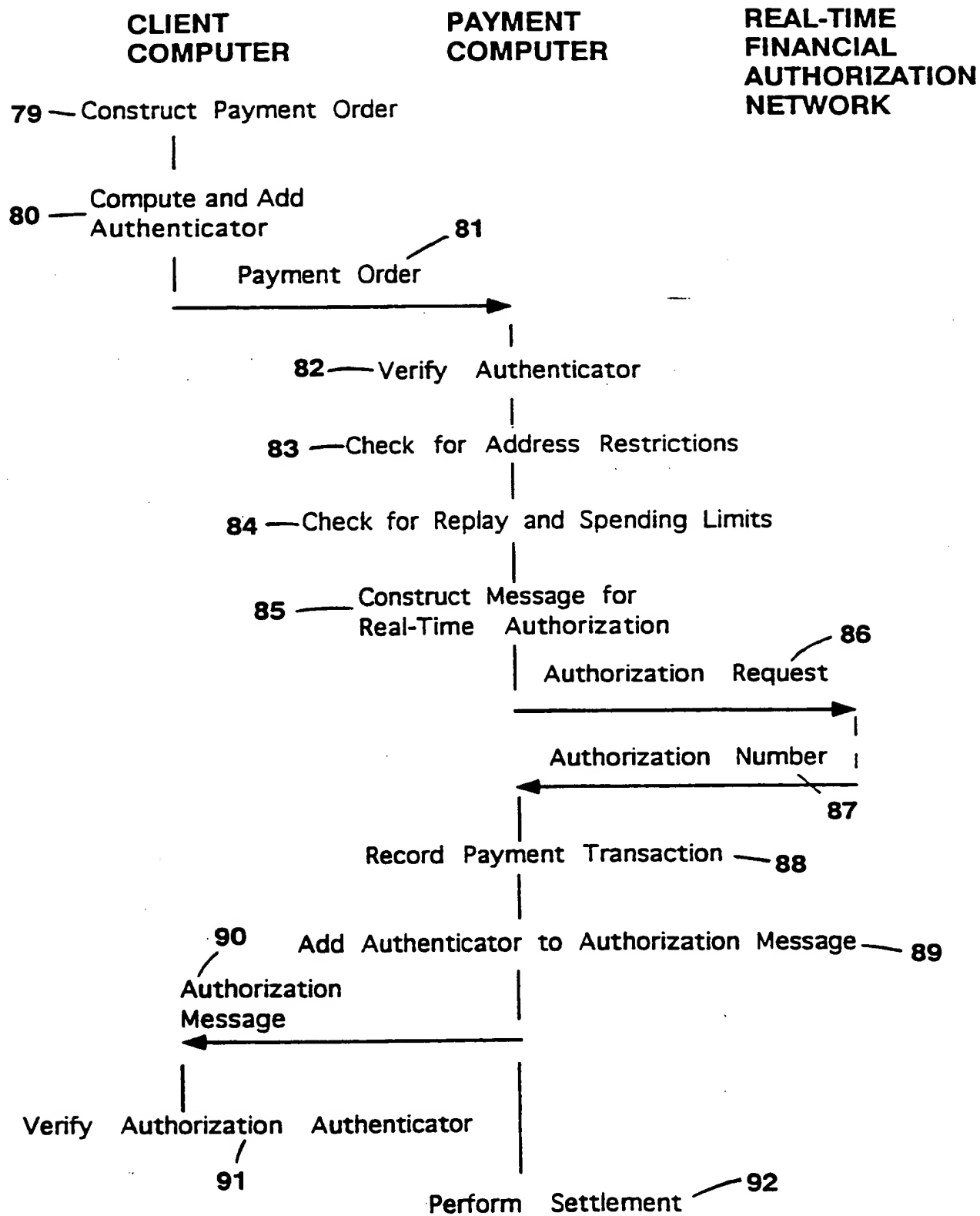
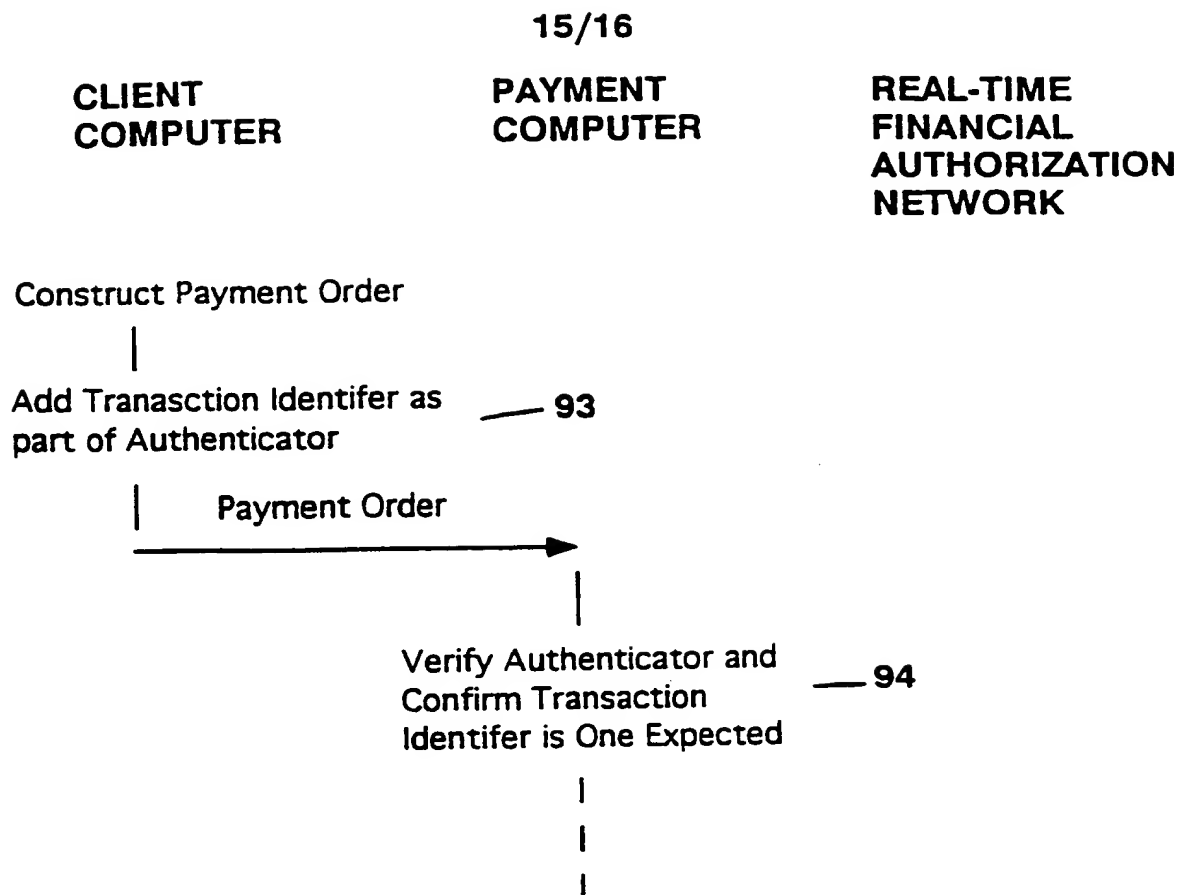


FIG. 14

**FIG. 15**

16/16

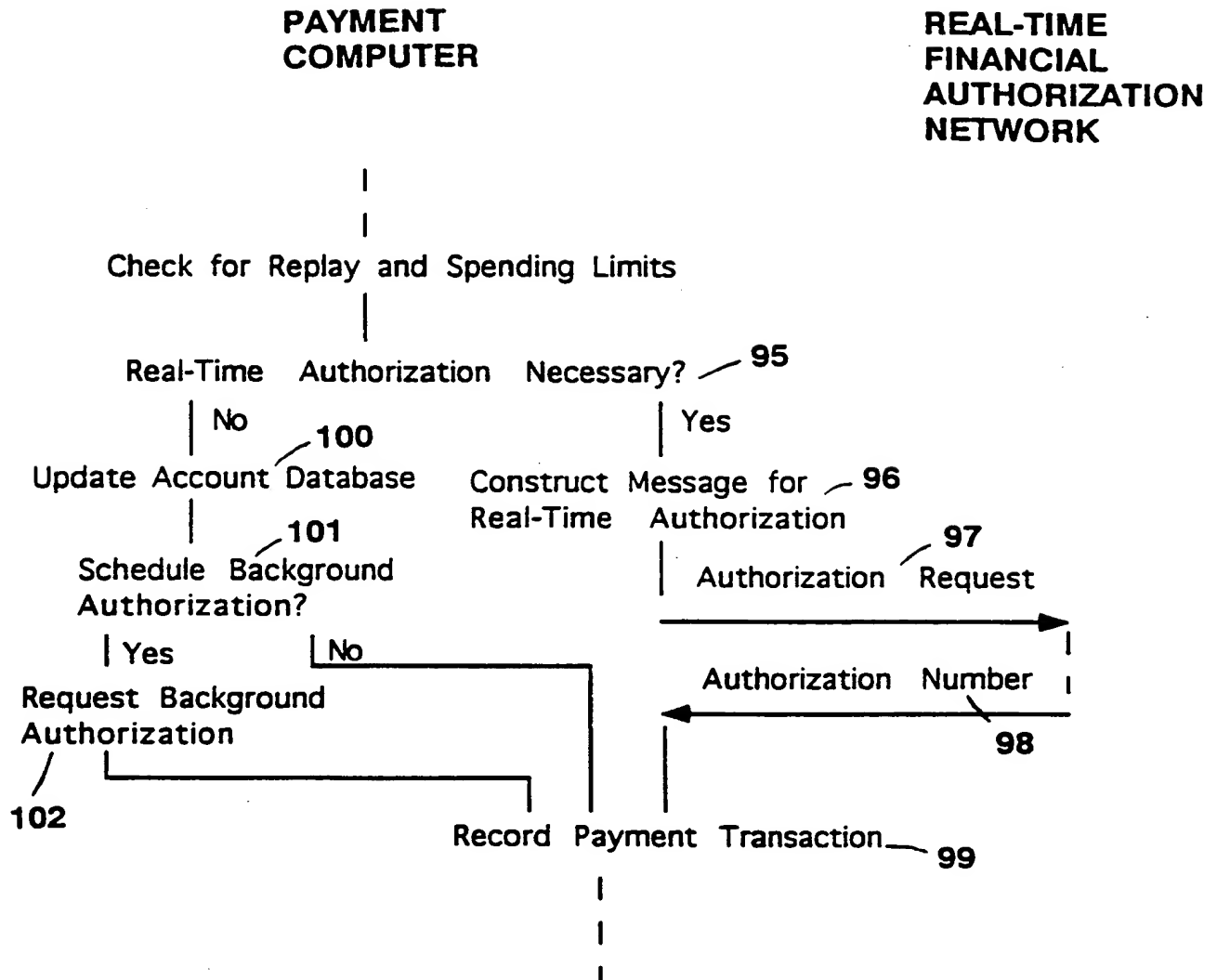


FIG. 16

INTERNATIONAL SEARCH REPORT

In national application No.
PCT/US94/14319**A. CLASSIFICATION OF SUBJECT MATTER**

IPC(6) :G06F 157:00

US CL :364/401,408

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 364/401, 406, 408; 340/825.33; 380/23, 24; 902/1, 2, 24

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
none

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS Database Search

Search terms include: home(2a)shop?, electronic?(2a)shop?, advertis?(p)program, download?(w)program?

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US, A, 4,799,156 (SHAVIT ET AL.) 17 January 1989, see entire document.	1-22
Y	US, A, 4,992,940 (DWORKIN) 12 February 1991, see col. 2, lines 30-34.	1-22
Y	US, A, 4,775,935 (YOURICK) 4 October 1988, see figures 5b and 6.	4, 15
Y	US, A, 4,935,870 (BURK, JR. ET AL.) 19 June 1990, see col. 15.	4, 15
Y	US, A, 5,025,373 (KEYSER, JR. ET AL.) 18 June 1991, see col. 4, lines 45-58, col. 6, lines 1-25, and col. 8, lines 39-45.	5, 8-9, 16, 19-20

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:	*T	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
A document defining the general state of the art which is not considered to be part of particular relevance	*X*	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
E earlier document published on or after the international filing date	*Y*	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
L document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	*A*	document member of the same patent family
O document referring to an oral disclosure, use, exhibition or other means		
P document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search

23 JANUARY 1995

Date of mailing of the international search report

01 MAY 1995

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized officer

DAVID M. HUNTLEY

Telephone No. (703) 305-9775

national application No.
PCT/US94/14319

PCT/US94/14319

[illegible]

THIS PAGE BLANK (USPTO)